



dsb

datenschutzbeauftragte
des kantons zürich

Informationssicherheit bei öffentlichen Internet-Terminals

Die Nutzung eines öffentlichen Internet-Terminals liegt grundsätzlich in der Verantwortung der Benutzerinnen und Benutzer. Dennoch muss das öffentliche Organ, das solche Terminals anbietet, angemessene organisatorische und technische Massnahmen vornehmen, um die Terminals zu schützen.

Dies bedingt zunächst, dass alle Internetzugänge über ein separates Netzsegment oder besser einen eigenen Internetanschluss erfolgen, damit kein Zugriff auf Informationen des öffentlichen Organs möglich ist.

Empfehlenswert ist, dass unerwünschte Seiten gesperrt und Nutzungsbestimmungen aufgestellt werden, etwa durch eine schriftliche Bekanntmachung. Die Nutzungsbestimmungen können sich beispielsweise an diejenigen der Verordnung über die Nutzung von Internet und E-Mail ([LS 177.115](#)) anlehnen. Weiter sollte die Nutzungsbestimmung folgende Punkte enthalten:

- Kurze Aufklärung über die Risiken im Internet
- Benennung einer Ansprechperson bei Sicherheitsproblemen
- Verbot zur Änderung der Konfigurationseinstellungen (z.B. Browser)

Zusätzlich zu den Standardsicherheitsmassnahmen wie Virenschutz, Firewall, Proxy, Updates sollten die Clients so eingerichtet sein, dass kein Zugriff auf die Daten des vorherigen Nutzers (Cookies, Browserverlauf, Texteingaben etc.) möglich ist. Mit Vorteil geschieht das Löschen der Nutzungsdaten mit einer technischen und automatisierten Lösung (zum Beispiel Löschen der Browserdaten beim Schliessen des Browsers oder Rücksetzung der Clients bei Neustart, keine Ablage temporärer Daten etc.). Im Idealfall geschieht dies über den Terminal-Modus des Betriebssystems. Steht keine technische Lösung zur Verfügung, so kann dies organisatorisch geregelt werden, indem die Benutzerinnen und Benutzer angewiesen werden, ihre Daten nach der Nutzung manuell zu löschen.

Aufgrund der vielen unterschiedlichen Personen, die ein öffentliches Internet-Terminal benutzen, sollen die Clients speziell abgesichert werden (unnötige Dienste deaktiviert, Benutzerberechtigungen stark eingeschränkt etc.), zum Beispiel darf sich keine Überwachungssoftware oder andere Schadsoftware durch die Benutzerinnen oder Benutzer installieren lassen. Dazu kann auch der Einsatz einer Internet-Terminal-Software hilfreich sein.

V 2.1 / März 2021